HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/717,761	11/21/2000	Xin Qiu	GIC-609	9034

7590 02/03/2005

Barry R Lipsitz
755 Main Street
Building No 8
Monroe, CT 06468

EXAMINER	
TRAN, TONGOC	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 02/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/717,761	QIU ET AL.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's application serial no. 09/717,761 file on 11/21/2000. Claims 1-48 are pending.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 3/5/2001 has been considered by the examiner.

Priority

3. Applicant's claim for domestic priority under 35 U.S.C. 119(e) has been acknowledged.

Claim Objections

4. Claims 20 and 44 are objected to because of the following informalities:

The ";" after the "steps of" and "comprising" appear to be typographical errors.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown (U.S. Patent No. 4,860,353) in view of Schneier ("Applied Cryptography, protocols, Algorithms, and Source Code in C", 1996).

In respect to claim 1, Brown discloses a method of generating a keystream, comprising the steps of providing data bits from predetermined register stages of multiple feedback shift registers to a first randomization stage, each feedback shift register having input, intermediate, and output stages through which the data bits are shifted serially in response to a clock signal; providing output of said first randomization stage to a second randomization stage; providing output of said second randomization stage and data bits from other predetermined register stages of said feedback shift registers to at least one additional randomization stage, and output of a final randomization stage provides said keystream (e.g. Fig. 1b, col. 1, line 50-col. 2, line 6). Brown does not disclose data bits are permutated at each randomization stage. However, Schneier discloses diffusion technique (through permutation) in stream ciphers to dissipate the redundancy of the plaintext by spreading it out over the ciphertext (page 237, 4th paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Brown's teaching of generating a keystream through multiple randomization stage to incorporate permutation of the data bits at each randomization stage in order to obscure the redundancy of the keystream (page 237, lines 10-11).

In respect to claim 2, Brown and Schneier disclose the method in accordance with claim 1, wherein a third randomization stage is the final randomization stage (Brown, col. 5, lines 14-33).

In respect to claim 3, Brown and Schneier disclose the method in accordance with claim 1, further comprising the step of:

varying at least one feedback shift register structure in response to a polynomial code signal generated by a polynomial code signal generator (Brown, col. 5, lines 14-33).

In respect to claim 4, Brown and Schneier disclose the method in accordance with claim 3, further comprising the step of: varying the polynomial code used to generate the polynomial code signal (Brown, col. 5, lines 44-54).

In respect to claim 5, Brown and Schneier disclose the method in accordance with claim 1, wherein the feedback shift registers comprise: a plurality of dynamic feedback shift registers; and at least one static feedback shift register (Brown, col. 3, lines 36-60 and col. 4, lines 3-25).

In respect to claim 6, Brown and Schneier disclose the method in accordance with claim 1, wherein the feedback shift registers comprise: a first dynamic feedback shift register; a second dynamic feedback shift register; and a static feedback shift register (Brown, col. 3, lines 36-60 and col. 4, lines 3-25).

In respect to claim 7, Brown and Schneier disclose the method in accordance with claim 6, further comprising the steps of: inputting seed data into an input buffer; providing a first portion of the seed data from the input buffer to the first feedback shift

register; providing a second portion of the seed data from the input buffer to the second feedback shift register; and providing a third portion of the seed data from the input buffer to the static feedback shift register (Brown, Fig. 1a and 1b, col. 4, line 25-col. 6, line 30).

In respect to claim 8, Brown and Schneier disclose the method in accordance with claim 7, wherein the data bits of the dynamic feedback shift registers are shifted serially from each register stage in response to a clock signal; a number of finite field adders are arranged between predetermined pairs of the register stages of the dynamic feedback shift registers, such that one of the inputs to each adder is provided from the preceding register stage and the other input of each adder is fed back from the output terminal of the output stage via a finite field multiplier (Brown, Fig. 1a and 1b, col. 4, line 25-col. 6, line 30).

In respect to claim 9, Brown and Schneier disclose the method in accordance with claim 1, wherein the first randomization stage comprises a randomization table for permuting data bits from predetermined register stages (Schneier, pages 271-278).

In respect to claim 10, Brown and Schneier disclose the method in accordance with claim 1, wherein the second randomization stage comprises a non-linear mixing function to combine the output of said second randomization stage and data bits from other predetermined register stages of said feedback shift registers (Schneier, page 412-413, section 17.6).

In respect to claim 11, Brown and Schneier disclose the method in accordance with claim 1, wherein the third randomization stage comprises multiple non-linear S-Boxes (Schneier, page 420, section 17.12).

In respect to claim 12, Brown and Schneier disclose the method in accordance with claim 11, wherein the S-Boxes are 8*8 S-Boxes (Schneier, page 400, section 17.3 and page 420, section 17.12).

In respect to claim 13, Brown and Schneier disclose the method in accordance with claim 1, wherein the third randomization stage comprises 256 non-linear 8*8 S-Boxes (Schneier, page 400, section 17.3 and page 420, section 17.12).

In respect to claim 14, Brown and Schneier disclose the method in accordance with claim 1, wherein the feedback shift registers are constructed using an extended Galois field ($GF(2^m)$) (Schneier, page 254, last paragraph-page 255 and page 378, 3rd paragraph-page 379, 2nd paragraph).

In respect to claim 15, Brown and Schneier disclose the method in accordance with claim 14, wherein m equals eight (Schneier, page 255).

In respect to claim 16, Brown and Schneier disclose the method in accordance with claim 14, wherein the polynomials used for the feedback shift registers are primitive and irreducible (Schneier, page 255).

In respect to claim 17, Brown and Schneier disclose the method in accordance with claim 1, wherein the first randomization stage comprises multiple randomization tables for permuting data bits from predetermined register stages (Schneier, pages 271-278).

In respect to claim 18, Brown and Schneier disclose the method in accordance with claim 17, wherein the multiple randomization tables comprise eight randomization tables (Schneier, pages 275-277).

In respect to claim 19, Brown and Schneier disclose the method in accordance with claim 1, further comprising the step of: multiplexing the data bits from the feedback shift registers prior to input into the first randomization stage (Brown, col. 4, lines 45-68).

In respect to claim 20, Brown and Schneier disclose the method in accordance with claim 1, further comprising the steps of; providing the output from the third randomization stage to a pre-keystream register; providing alternate bits of the output from said pre-keystream register to a select chain buffer; providing output from the select chain buffer to a decoding logic unit, which decoding logic unit decodes a particular polynomial for use in generating a polynomial code signal, said polynomial code signal being provided to at least one feedback shift register; and providing the remaining bits of the output from said pre-keystream register to a keystream register, wherein the output of the keystream register provides said keystream (Brown, Fig. 1b and col. 4, line 25-col. 5, line 43).

In respect to claim 21, Brown and Schneier disclose the method in accordance with claim 20, wherein the third randomization stage comprises multiple non-linear S-Boxes (Schneier, pages 275-276 and page 412-413, page 420).

In respect to claim 22, Brown and Schneier disclose the method in accordance with claim 21, further comprising the steps of: providing certain output of the S-Boxes to a codestream register; clocking said output through said codestream register; adding

said output to data bits shifted from at least one of the feedback shift registers via a nonbinary adder to produce feedback data bits; providing the feedback data bits to the input stage and predetermined intermediate stages of at least one of the feedback shift registers (Schneier, pages 372, section 16.2 and 17.3).

In respect to claim 23, Brown and Schneier disclose the method in accordance with claim 1, wherein a 192 bit shared seed input key is provided to the multiple feedback shift registers; and a 56 bit keystream output is generated (Schneier, pages 166-167, 175 and 283).

In respect to claim 24, Brown and Schneier disclose the method in accordance with claim 23, wherein the 192 bit shared seed input key is derived from a 128 bit input by duplicating half the bits (Schneier, pages 166-167, 175 and 283).

In respect to claims 25-48, the claim limitations are apparatus claims that are substantially similar to the method claims 1-24. Therefore, claims 25-48 are rejected based on the similar rationale.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Driscoll discloses a computer efficient linear feedback shift register.

-Rose (2002/0015493, 2003/0206634) discloses method and apparatus for generating encryption stream ciphers.

-Venkatesan et al. Disclose lightweight word-oriented technique for generating pseudo-random sequence for use in keystream of a stream cipher.

-Aiello et al. (5,727,063, 5,515,307)Disclose method for generating pseudo-random bitstream.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

TT
December 3, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100